Приложение №3 к Техническому заданию

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

**на выполнение работ по созданию подсистемы защиты информации автоматизированной информационной системы управления фондом капитального ремонта регионального оператора города Севастополя**

1. **Общие сведения**
   1. **Объект защиты**

Информационная система персональных данных (далее ИСПДн) – автоматизированная информационная система управления фондом капитального ремонта регионального оператора города Севастополя.

* 1. **Состав работ**

Работы по созданию подсистемы включают в себя:

## поставку программного и аппаратного обеспечения средств защиты информации и технических средств;

## выполнение монтажа и настройки программного и аппаратного обеспечения средств защиты информации и технических средств.

* 1. **Основание проведения работ**

Основаниями проведения настоящих работ являются:

## наличие у Заказчика ИСПДн, в которых осуществляется обработка персональных данных сотрудников Заказчика и граждан, пользующихся услугами Заказчика (далее - субъекты персональных данных);

## требования законодательства Российской Федерации в области обработки и защиты персональных данных.

1. **Назначение и цели создания подсистемы защиты объектов информатизации**
   1. **Назначение подсистемы защиты**

Подсистема защиты персональных данных ИСПДн предназначена для обеспечения выполнения требований Федеральной службы по техническому и экспортному контролю России (далее - ФСТЭК России), Федеральной службы безопасности Российской Федерации (далее – ФСБ РФ) и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор).

* 1. **Цели создания подсистемы защиты объектов информатизации**

Основными целями создания подсистемы защиты персональных данных ИСПДн являются:

## защита персональных данных субъектов, обрабатываемых техническими средствами, от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа за счёт комплексного использования организационных, программных, программно-аппаратных средств и мер защиты;

## защита персональных данных, передаваемых по открытым каналам связи, от утечки, искажения и подмены авторства сообщения;

## выполнение требований ФСТЭК России, ФСБ РФ и Роскомнадзора по защите персональных данных.

1. **Общая характеристика объектов информатизации**

В состав ИСПДн Заказчика входят:

## 10 АРМ под управлением ОС семейства Windows.

## Сервер Системы, расположенный в центре обработки данных Исполнителя.

1. **Требования к подсистеме защиты персональных данных**
   1. **Требования законодательства в сфере защиты персональных данных**

Для объектов информатизации Заказчика мероприятиями по защите персональных данных, обрабатываемых на объектах информатизации Заказчика, будут являться меры, соответствующие выполнению требований:

## Федерального закона РФ № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»;

## Федерального закона РФ № 152-ФЗ от 27 июля 2006 г. «О персональных данных»;

## Постановления Правительства Российской Федерации № 211 от 21 марта 2012 г. «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

## Постановления Правительства Российской Федерации № 1119 от 01 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

## нормативно-методических документов ФСТЭК РФ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

## нормативно-методических документов ФСБ РФ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

* 1. **Требования к подсистеме защиты в целом**

Для реализации мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, Исполнитель должен создать подсистему защиты персональных данных ИСПДн.

* + 1. **Требования к структуре и функционированию подсистемы защиты персональных данных ИСПДн**
       1. **Требования к составу**

Для создания подсистемы необходимо построить следующие подсистемы, используя поставляемые Исполнителем программное и аппаратное обеспечение в соответствии с разделом 5 настоящего Технического задания:

## подсистема управления доступом, регистрации, учета и обеспечения целостности;

## подсистема межсетевого экранирования и защиты каналов связи;

## подсистема обнаружения вторжений;

## подсистема антивирусной защиты.

* + - * 1. **Подсистема управления доступом, регистрации, учета и обеспечения целостности**

Описываемая подсистема должна включать в себя средство управления доступом субъектов доступа к объектам доступа - СЗИ от НСД Dallas-Lock 8.0-С.

Все АРМ Заказчика, участвующие в обработке персональных данных, должны быть оснащены Исполнителем средствами управления доступа пользователей.

* + - * 1. **Подсистема межсетевого экранирования и защиты каналов связи**

Описываемая подсистема должна включать в себя следующие компоненты:

## Программное обеспечение для управления защищенной сетью в составе: ПО ViPNet Administrator, ПК для развертывания ПО ViPNet Administrator, СЗИ НСД Аккорд.

## Программно-аппаратный комплекс ПАК VipNet HW1000 в количестве 1 ед.

## персональный межсетевой экран с встроенной защитой каналов связи - ПО ViPNet Client 3.х (КС2).

Все АРМ Заказчика, участвующие в обработке персональных данных, должны быть оснащены Исполнителем персональным межсетевым экраном.

* + - * 1. **Подсистема обнаружения вторжений**

Описываемая подсистема должна включать в себя систему обнаружения вторжений - Security Studio Endpoint Protection: Antivirus, Personal Firewall, HIPS.

Все АРМ Заказчика, участвующие в обработке персональных данных, должны быть оснащены Исполнителем системой обнаружения вторжений.

* + - * 1. **Подсистема антивирусной защиты**

Описываемая подсистема должна включать в себя средство антивирусной защиты - Security Studio Endpoint Protection: Antivirus, Personal Firewall, HIPS.

Все АРМ Заказчика, участвующие в обработке персональных данных, должны быть оснащены Исполнителем средством антивирусной защиты.

* + - 1. **Требования к взаимосвязи между подсистемами и компонентами, смежными подсистемами**

Смежными подсистемами являются:

## локальная вычислительная сеть;

## сеть международного информационного обмена – Интернет.

Решения по подключению смежных подсистем должны соответствовать действующим государственным стандартам в области связи и телекоммуникаций.

* + 1. **Показатели назначения подсистемы защиты ИСПДн**
       1. **Подсистема управления доступом, регистрации, учёта и обеспечения целостности**

Средство управления доступом пользователей должно обеспечить выполнение политики управления доступом, разграничения прав доступа, парольной политики Заказчика, контроль целостности средств защиты информации на АРМ Заказчика.

* + - 1. **Подсистема межсетевого экранирования и защиты каналов связи**

Программное и аппаратное обеспечение подсистемы межсетевого экранирования и защиты каналов связи должно защищать АРМ от сетевых атак и попыток несанкционированного доступа при подключении к сети, а так же должно:

## осуществлять фильтрацию защищенного и открытого трафиков по множеству параметров;

## осуществлять контроль доступа в сеть приложений;

## осуществлять построения шифрованного VPN туннеля.

* + - 1. **Подсистема обнаружения вторжений**

Система обнаружения вторжений должна обеспечивать блокировку вредоносных процессов при их попытках воздействия на рабочие процессы АРМ.

* + - 1. **Подсистема антивирусной защиты**

Средство антивирусной защиты должно защищать АРМ от воздействий вредоносного программного обеспечения.

* + 1. **Требования к надёжности**

Элементы подсистемы защиты ИСПДндолжны удовлетворять условию круглосуточной работы, а также иметь возможность восстановления в случаях сбоев.

* 1. **Требования к организационному обеспечению**

Исполнителем должны быть разработаны необходимые технические и организационно-распорядительные документы по защите персональных данных в соответствии с требованиями федеральных законов, документов ФСТЭК России, ФСБ России.

Документация должна соответствовать требованиям следующих руководящих документов в области обеспечения обработки и защиты информации:

## Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

## Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных» (ред. от 25.07.2011);

## Федеральный закон от 27.07.2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

## Указ Президента Российской Федерации от 6.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

## Постановление Правительства РФ от 15.09.2008 г. № 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

## Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

## Постановление Правительства РФ от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

## Постановление Правительства РФ от 21 03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

## Приказ ФСТЭК РФ от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

## Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Председателя Гостехкомиссии России от 30.08.2002 г. № 282;

## Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования по защите информации» (РД АС);

## Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

## Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

## Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (введен в действия Приказом Председателя Гостехкомиссии России № 114 от 04.06.1999 г.);

## Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15.02.2008 г.;

## Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 14.02.2008 г.;

## Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные 8 Центром ФСБ России от 21.02.2008 г. № 149(54-144);

## Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством 8 Центра ФСБ России 21.02.2008 г. 112 149/6/6-622.

Перечень разрабатываемых документов:

## Приказ о назначении администратора информационной безопасности.

## Приказ о назначении ответственного пользователя средств криптографической защиты информации.

## Приказ об определении границ контролируемой зоны ИСПДн

## Приказ об утверждении перечня персональных данных, обрабатываемых в ИСПДн.

## Приказ об утверждении перечня помещений, в которых осуществляется обработка персональных данных в ИСПДн

## Приказ об утверждении перечня сотрудников, имеющих право доступа к информации, обрабатываемой в ИСПДн

## Приказ об утверждении перечня должностей, сотрудников, замещение которых предусматривает осуществление обработки персональных данных в ИСПДн

## Приказ об утверждении перечня должностей сотрудников, ответственных за проведение мероприятий по обезличиванию персональных данных, обрабатываемых в ИСПДн.

## Приказ об утверждении Положения по организации и проведению работ по обеспечению безопасности персональных данных, включающее:

## инструкцию администратора информационной безопасности;

## инструкцию пользователя ИСПДн;

## первичный инструктаж лица, допущенного к работе с персональными данными;

## порядок взаимодействия по вопросам обеспечения безопасности персональных данных;

## ответственность за нарушение требований законодательства;

## правила внутреннего контроля соответствия обработки персональных данных в ИСПДн требованиям к защите персональных данных;

## порядок приостановления предоставления персональных данных пользователям ИСПДн при обнаружении нарушений порядка предоставления персональных данных;

## порядок проведения служебных проверок по фактам нарушения требований по обеспечению безопасности персональных данных;

## порядок обезличивания персональных данных;

## порядок уничтожения персональных данных;

## порядок работы с электронными журналами ИСПДн;

## инструкцию по организации мер антивирусной защиты в ИСПДн;

## инструкцию по организации парольной защиты в ИСПДн;

## инструкцию по порядку обращения со средствами защиты информации в ИСПДн;

## инструкцию по резервированию и восстановлению информации в ИСПДн;

## инструкцию по учету машинных носителей информации ИСПДн;

## инструкцию по обработке персональных данных без использования средств автоматизации в ИСПДн;

## инструкцию по криптографической защите информации в ИСПДн

## Приказ о назначении комиссии для проведения оценки вреда субъектам персональных данных

## Приказ о назначении комиссии по определению уровня защищенности персональных данных,

## Приказ об утверждении перечня средств криптографической защиты информации, их мест размещения и их пользователей

## Матрица доступа пользователей к защищаемым информационным ресурсам ИСПДн.

## Модель угроз ИСПДн.

## Акт классификации ИСПДн по требованиям безопасности

## Акт оценки вреда субъектам персональных данных, чьи персональные данных обрабатываются в ИСПДн

## Требования по обеспечению безопасности персональных данных при их обработке в ИСПДн.

## Описание технологического процесса обработки персональных данных в ИСПДн.

## Описание системы защиты персональных данных в ИСПДн.

## Технический паспорт ИСПДн

* 1. **Требования к техническому сопровождению**

Все поставляемые средства защиты информации должны быть обеспечены техническим сопровождением в течении 1 года, включающим в себя оказание технических консультаций сертифицированными специалистами Исполнителя, по вопросам функционирования средств защиты информации по телефону горячей линии в течение рабочего дня Заказчика (с 09:00 до 18:00, с понедельника по пятницу) и электронной почте.

* 1. **Требования к гарантийному обслуживанию**

Все поставляемые средства защиты информации должны быть обеспечены гарантийным обслуживанием в течение 1 года.

* 1. **Требования по обеспечению конфиденциальности проводимых работ**

Исполнитель работ обязуется:

## не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся на объектах информатизации Заказчика;

## не осуществлять несанкционированный доступ к информационным ресурсам Заказчика;

## не предпринимать манипулирование информацией, циркулирующей или хранящейся на объектах информатизации Заказчика (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);

## не проводить незаконное копирование информации, циркулирующей или хранящейся на объектах информатизации Заказчика;

## не нарушать технологию сбора, накопления, ввода, вывода, приема, передачи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;

## не устанавливать программное обеспечение, зараженное вирусами, программные и аппаратные закладные устройства в технические средства Заказчика;

## не внедрять на объекты информатизации Заказчика программы-вирусы (загрузочные, файловые и др.);

## не распространять конфиденциальную информацию о настоящих работах и полученных результатах.

Нарушение настоящих требований влечет за собою гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

**5. Спецификация поставляемых средств защиты информации и объем выполняемых работ**

| **№**  **п/п** | **Наименование поставляемых средств защиты информации (выполняемых работ)** | **Характеристики поставляемых средств защиты информации**  **(выполняемых работ)** | **Объем поставки/работ** | |
| --- | --- | --- | --- | --- |
| **Единица измерения** | **Кол-во** |
|  | Право на использование ПО ViPNet Administrator 3.х (КС2) | Программное обеспечение должно реализовывать функции управления защищенной сетью и соответствовать следующим критериям:   * состоять из центра управления сетью и ключевого удостоверяющего центра; * быть полностью совместимым с поставляемым ПАК ViPNet Coordinator HW1000 и ПО ViPNet Client; * вырабатывать ключи, соответствующие ГОСТ 28147–89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001; * создавать узлы защищенной сети (криптографические шлюзы и клиенты), удалять узлы защищенной сети, определять политику связей защищенных узлов между собой, определять политику безопасности и формировать списки прикладных задач для узлов защищенной сети; * производить автоматическую рассылку справочной и ключевой информации; * проводить автоматическое обновление программного обеспечения криптошлюзов и криптографических клиентов; * формировать симметричные ключи связи узлов (криптошлюзы и криптографические клиенты) между собой; * формировать сертификаты электронно-цифровой подписи формата Х.509v.3; * вести списки отозванных сертификатов электронно-цифровой подписи; * наличие модуля гарантированной доставки обновления справочно-ключевой информации на криптошлюзы и криптографические клиенты; * соответствие требованиям ФСБ России должен к средствам криптографической защиты информации класса КС2. | лицензия | 1 |
|  | Персональный компьютер для ViPNet Administrator | Поставляемый персональный компьютер должен обладать характеристиками не ниже следующих:  1 процессор с 2 ядрами и тактовой частотой не менее 2,6 ГГц, 2 Гб оперативной памяти, жесткий диск 500 Гб, привод DVD-RW, сетевой адаптер Fast Ethernet, монитор LCD 19", клавиатура, мышь, предустановленная ОС Windows 7 Professional, источник бесперебойного питания | шт. | 1 |
|  | СЗИ НСД для ViPNet Administrator | Комплекс СЗИ НСД. Сертифицированный ФСБ России. | шт. | 1 |
|  | ПАК ViPNet Coordinator HW1000 | ПАК должен реализовывать функции криптографического шлюза и отвечать следующим требованиям:   * быть полностью совместимым с поставляемым программным обеспечением, реализующим функции управления защищенной сетью: обновление программного обеспечения, обновление справочно-ключевой информации, управление политиками безопасности; * иметь предустановленную операционную систему; * иметь не менее четырех сетевых интерфейсов 100/1000 Mbit; * алгоритм шифрования должен соответствовать ГОСТ 28147-89 (256 бит); * иметь форм фактор 1 U для размещения в одном слоте серверного шкафа; * иметь сертификат ФСТЭК России по требованиям к межсетевым экранам по 3 классу, по отсутствию недекларируемых возможностей по 3 уровню контроля, с возможностью использования при создании автоматизированных систем класса защищенности до 1В включительно; * иметь сертификат ФСБ России по требованиям к СКЗИ не ниже класса КС2; * иметь встроенное программное обеспечение, реализующее функции криптографического шлюза; * позволять осуществлять функции прокси-сервера защищенных соединений; * позволять предоставлять функции туннелирующего сервера без ограничения числа тунеллируемых IP-адресов; * позволять предоставлять функции сервера IP-адресов (регистрация и предоставление информации о текущих IP-адресах и состоянии объектов защищенной сети); * программное обеспечение, реализующее функции криптографического шлюза, должно использовать IP-адресацию для организации защищенных каналов связи с другими криптографическими шлюзами, основанную на шестнадцатеричных идентификаторах; * программное обеспечение, реализующее функции криптографического шлюза, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищенной сетью. | шт. | 1 |
|  | Право на использование ПО ViPNet Client 3.х (КС2) | Программное обеспечение должно реализовывать функции криптографического клиента, а также отвечать следующим требованиям:   * совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью (ViPNet Administrator), обновления программного обеспечения, обновления справочно-ключевой информации, управление политиками безопасности; * совместимо (полностью) с программно-аппаратным комплексом, реализующим функции шифрование/дешифрование направляемого/принимаемого IP-трафика (ViPNet Coordinator HW1000); * поддержка операционных систем:   • Microsoft Windows 2000 Professional;  • Microsoft Windows XP Home/Professional;  • Microsoft Windows Vista (вся линейка);  • Microsoft Windows 7 (вся линейка).   * наличие сертификата ФСТЭК России по требованиям к межсетевым экранам по 3 классу, отсутствию не декларируемых возможностей по 3 уровню, иметь ОУД не ниже 4+ и возможностью использования в АС до класса 1В включительно; * наличие сертификата ФСБ России по классу КС1/КС2; * предоставлять функции контроля запускаемых в операционной системе приложений; * предоставлять функции контентной фильтрации прикладных протоколов http, ftp; * программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью; * -взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»). | лицензия | 10 |
|  | СЗИ от НСД Dallas-Lock 8.0-С | СЗИ от НСД должна представлять собой программный комплекс средств защиты информации в операционных системах семейства Windows с возможностью подключения аппаратных идентификаторов.  СЗИ от НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2 в многопользовательском режиме их эксплуатации.  СЗИ НСД должна поддерживать 32- и 64-битные версии операционных систем.  СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go.  СЗИ НСД должна быть сертифицирована по требованиям Руководящих документов (РД) ФСТЭК России (Гостехкомиссии России) по 3 классу защиты от НСД для СВТ и 2 уровню контроля отсутствия НДВ, разрабатываться и производиться на основании лицензии органов, имеющих федеральные полномочия в указанной сфере.  СЗИ НСД может быть использована при создании защищенных автоматизированных систем до класса защищенности 1Б включительно, для обеспечения 1 уровня защищенности персональных данных и в государственных информационных системах 1 класса защищённости.  СЗИ НСД должна обеспечивать:   * Регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере. * Идентификацию и проверку подлинности пользователей при входе в операционную систему, а также аутентификацию при входе на ПЭВМ до начала загрузки ОС. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows. * Реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам. * Должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), реестру, сети, съемным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных. * Для предотвращения утечки информации с использованием съемных носителей информации СЗИ НСД должна позволять разграничивать доступ как к отдельным типам носителей, так и к конкретным экземплярам. Возможность настройки мандатного доступа к устройствам. | шт. | 10 |
|  | Право на использование Средств защиты информации Security Studio Endpoint Protection: Antivirus, Personal Firewall, HIPS. (срок действия – 1 год) | ***Должен осуществлять:***   * межсетевое экранирование для автоматизированного рабочего места в сетях TCP/IP; * защиту компьютера от атак по сети TCP/IP; * антивирусную защиту от вредоносного программного обеспечения; * защиту от спама и вредоносного контента веб-серверов; * самозащиту от воздействия со стороны вредоносного программного обеспечения; * регистрацию событий безопасности; * иметь соответствующие сертификаты ФСТЭК. * функции программного средства защиты информации, предназначенного для обнаружения вторжений.   ***Требования к поддержке операционных платформ***:   * Windows 8, 7, Vista, XP x86/x64; Windows Server 2012 x64; Windows Server 2008 R2 x64, Server 2008 x86/x64;Windows Server 2003 R2 x86/x64, Server 2003 x86/x64;   ***Требования к функциональности:***   * должно контролировать входящие и исходящие соединения; * должно обеспечивать контроль для приложений, использующихся на компьютере, при обращении к сети и создание правил сетевого доступа для приложений; * режим обучения для сетевого доступа для приложений; * разделение доступа к узлам сети; * создание разрешенного и запрещенного списков сетевых ресурсов; * возможность экспорта/импорта настроек межсетевого экрана с одного компьютера на другой; * должно обеспечивать блокировку активного содержимого страниц веб-серверов; * должно обеспечивать блокировку активного содержимого входящих электронных писем; * должно обеспечивать настройку на обнаружение типовых сетевых атак; * должно обеспечивать блокировку сетевых сканеров; * должно обеспечивать блокировку вредоносных процессов при их попытках воздействия на рабочие процессы; * должно обеспечивать непрерывный мониторинг; * должно обеспечивать регистрацию событий безопасности.   ***Требования по сертификации:***   * должно иметь сертификат ФСТЭК в соответствии с руководящим документом "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" (Гостехкомиссия России, 1997) не ниже, чем по 4-му классу защищенности. * должно являться программным средством защиты информации, предназначенным для обнаружения вторжений из внешних вычислительных сетей; * должно соответствовать требованиям документа «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) – по 4 классу защиты, «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012) – не ниже, чем по 4 классу защиты. | лицензия | 10 |
|  | Установочный комплект Security Studio Endpoint Protection | Компакт диск с программным обеспечением, формуляр. | шт. | 1 |
|  | Установочный комплект VipNet | Компакт диск с программным обеспечением, формуляр. | шт. | 1 |
|  | Право на использование программного средства ведения журналов учета в электронном виде ПО «КИТ-Журнал» | Должно обладать следующими характеристиками:  - поддержка сертифицированных криптопровайдеров для создания электронной подписи (в том числе ViPNet CSP);  - поддержка шаблонов записей;  - наличие встроенного планировщика;  - возможность изменения форм;  - возможность вывода электронных журналов на печать;  - разграничение прав пользователей к электронным журналам;  - должно быть зарегистрировано в государственном реестре программ и баз данных в соответствии с действующим законодательством как самостоятельная программа для ЭВМ;  - должно функционировать независимо от прочих средств защиты информации, требуемых в соответствии с настоящей конкурсной документацией;  - должно иметь клиент-серверную архитектуру, с возможностью последующего добавления клиентских лицензий;  - наличие встроенной службы штампов времени, с применением электронной подписи для подтверждения подлинности штампов;  - наличие встроенной службы резервирования, с возможностью создания и редактирования собственных политик резервирования;  - средство должно содержать встроенный редактируемый типовой комплект журналов учета по информационной безопасности;  - наличие механизма пользовательских операций-сценариев, реализующих наглядный пользовательский режим работы средства учета;  - наличие встроенных средств поиска и фильтрации в электронных журналах;  - поддержка графических планшетов собственноручной подписи. | шт. | 1 |
|  | Сертификат технической поддержки СЗИ ViPNet на 1 год | Сертификат должен распространятся на приобретаемые средства защиты информации.  Состав услуг в сертификате:  Оказание технических консультаций сертифицированными специалистами, с привлечением специалистов производителя средств защиты по вопросам функционирования средств защиты информации по телефону горячей линии в течение рабочего дня (с 09:00 до 18:00, с понедельника по пятницу) и по электронной почте.  Техническая поддержка должна быть подтверждена сертификатом производителя программного обеспечения ViPNet (ОАО «ИнфоТеКС») | шт. | 1 |
|  | Сертификат технической поддержки СЗИ Dallas Lock на 1 год | Сертификат должен распространятся на приобретаемые средства защиты информации.  Состав услуг в сертификате:  Оказание технических консультаций сертифицированными специалистами, с привлечением специалистов производителя средств защиты по вопросам функционирования средств защиты информации по телефону горячей линии в течение рабочего дня (с 09:00 до 18:00, с понедельника по пятницу) и по электронной почте.  Техническая поддержка должна быть подтверждена сертификатом производителя программного обеспечения Dallas Lock (ООО "Конфидент") | шт. | 1 |
|  | Сертификат технической поддержки Security Studio Endpoint Protection на 1 год | Сертификат должен распространятся на приобретаемые средства защиты информации.  Состав услуг в сертификате:  Оказание технических консультаций сертифицированными специалистами, с привлечением специалистов производителя средств защиты по вопросам функционирования средств защиты информации по телефону горячей линии в течение рабочего дня (с 09:00 до 18:00, с понедельника по пятницу) и по электронной почте.  Техническая поддержка должна быть подтверждена сертификатом производителя программного обеспечения Security Studio Endpoint Protection (ООО "Код безопасности") | шт. | 1 |
|  | Установка и настройка ПО ViPNet Administrator 3.х (КС2) | Должна быть произведена установка и настройка средств защиты информации в соответствии с требованиями эксплуатационной документации и требований Заказчика | ед. | 1 |
|  | Установка и настройка ПАК ViPNet Coordinator HW1000 | Должна быть произведена установка и настройка средств защиты информации в соответствии с требованиями эксплуатационной документации и требований Заказчика | ед. | 1 |
|  | Установка и настройка ПО ViPNet Client 3.х (КС2) | Должна быть произведена установка и настройка средств защиты информации в соответствии с требованиями эксплуатационной документации и требований Заказчика | ед. | 10 |
|  | Установка и настройка Dallas-Lock | Должна быть произведена установка и настройка средств защиты информации в соответствии с требованиями эксплуатационной документации и требований Заказчика | ед. | 10 |
|  | Установка и настройка Security Studio Endpoint Protection | Должна быть произведена установка и настройка средств защиты информации в соответствии с требованиями эксплуатационной документации и требований Заказчика | ед. | 10 |
|  | Установка и настройка программного средства ведения журналов учета в электронном виде ПО «КИТ-Журнал» | Должна быть произведена установка и настройка средств защиты информации в соответствии с требованиями эксплуатационной документации и требований Заказчика | ед. | 1 |
|  | Разработка пакета технической и организационно-распорядительной документации по защите персональных данных в соответствии с требованиями федеральных законов, документов ФСТЭК России, ФСБ России | В соответствии с требованиями нормативно-технических документов | ед. | 1 |